REMARKS

Claims 1-2, 4-8, 10-14 and 16-18 were examined by the Office, and in the final Office Action of April 26, 2010 all claims are rejected. With this response, claims 1, 7 and 13 are amended. All amendments are fully supported by the specification as originally filed. Support for the amendments can be found at least from page 5, lines 21-24 and page 12, lines 3-10. Applicant respectfully requests reconsideration and withdrawal of the rejections in view of the following discussion.

This response is submitted along with a Request for Continued Examination (RCE).

**Claim Rejections Under § 103**

On page 2 of the Office Action, claims 1-2, 4-8, 10-14 and 16-18 are rejected under 35 U.S.C. § 103(a) as unpatentable over Morgan (U.S Patent No. 6,968,459) in view of Grawrock (U.S. Appl. Publ. No. 2003/0196100). Applicant respectfully submits that claim 1 is not disclosed or suggested by the cited references, alone or in combination, because the cited references fail to disclose or suggest all of the limitations recited in claim 1. The cited references at least fail to disclose or suggest that the second processor operating mode is set when testing or debugging is performed. Furthermore, claim 1 recites that the storage area in the storage circuit has protected data relating to security functions of the circuitry and protected applications. In addition, depending upon the processor operating mode, the processor may or may not have access to the storage area in which the protected data is located. Therefore, according to claim 1, the processor may or may not have access to protected data relating to security functions of the circuitry, depending upon which processor operating mode is set. This is in contrast to the information loaded or accessed from a removable storage device as in Morgan.

Claim 1 is amended to recite that the second processor operating mode is set when testing or debugging is performed. Both Morgan and Grawrock are silent with respect to setting a second operating mode when testing or debugging is performed. In Morgan, the restricted-access mode is operated when the computer senses a non-secure removable storage device. See Morgan column 1, lines 39-42. However, if the computer detects device-specific security information on the storage device, then the computer automatically operates in full-access data storage mode. See Morgan column 4, lines 47-49. If the storage manager is unable to retrieve drive-specific information, the storage manager then operates the computer in the restricted-

access data storage mode. See Morgan column 5, lines 35-38. The storage manager operates the computer in restricted-access mode by default until the storage manager has successfully initialized and verified the storage devices. See Morgan column 7, lines 27-30. Therefore, in Morgan whether the computer is in restricted-access or open-access mode depends upon whether secure or non-secure removable storage devices are attached to the computer. In contrast to Morgan, claim 1 recites that the second processing operating mode is set when testing or debugging is performed. Since the setting of access modes in Morgan is dependent upon the storage device attached to the computer, Morgan fails to disclose or suggest setting operating modes when testing or debugging is performed, as recited in claim 1. Grawrock is also silent regarding setting operating mode when testing or debugging is performed, and therefore fails to make up for the deficiencies in the teachings of Morgan identified above. Therefore, for at least the reasons discussed above claim 1 is not disclosed or suggested by the cited references.

In addition, in Morgan, one or more removable media drives (121) are used to access one or more removable storage devices (151), and each storage device has a storage medium for holding digital information. See Morgan column 3, lines 5-10. In order to automatically detect whether a storage device (151) is a secure device, computer (100) determines whether device-specific security information was written to storage device (151). See Morgan column 4, lines 6-9. The computer (100) is configured to operate in a restricted-access mode upon power-up until removable storage device (151) is verified as secure, and a secure computing environment is provided when the user tries to boot directly from one of the removable storage devices (151). See Morgan column 7, lines 17-24. However, the storage devices (151) do not contain protected data that relates to the security functions of the circuitry, as recited in claim 1. This is because the storage devices (151) contain a variety of digital information that is dependent upon the storage device, i.e. whether it is a secure storage device or a non-secure storage device. Accordingly, claim 1 recites that the storage area of claim 1 contains the same protected data, and access to the storage area is dependent upon which operating mode the processor is set in. Therefore, for at least this reason, claim 1 is not disclosed or suggested by the cited references.

In addition, the Office relies upon Grawrock to disclose storage circuit access control means arranged to prevent the processor from accessing the storage area in which protected data are located, and asserts that Grawrock discloses the AC module contained in private memory that is accessible when privileges and modes are set. However, Grawrock does not disclose or

suggest that the AC module contains protected data related to the security functions of the circuitry, as recited in claim 1. Instead, Grawrock only discloses that the AC modules are authenticated code modules. See Grawrock paragraph [0015]. In contrast to claim 1, Grawrock discloses that the processor (102) may include a key (118) that may be used by the processor to authenticate an AC module prior to executing the AC module. See Grawrock paragraph [0016]. Therefore, the AC module cannot contain protected data related to the security functions of the circuitry, because the AC module must be authenticated using the key (118) prior to the processor (102) executing the AC module. While Grawrock discloses that certain regions of the memory (108) may be defined as security enhanced (SE) memory, and that the processor (102) may only access SE memory (122) when in an appropriate operating mode and privilege level, Grawrock is silent regarding that the SE memory contains protected data related to the security functions of the circuitry, as recited in claim 1. Therefore, it is irrelevant that Grawrock may disclose that a memory controller (120) denies untrusted access to the system memory, because as discussed above with Morgan, Grawrock does not disclose or suggest protected data related to the security functions of the circuitry. Accordingly, for at least this reason, claim 1 is not disclosed or suggested by the cited references.

Independent claims 7 and 13 include limitations similar to those recited in claim 1. Therefore, independent claims 7 and 13 are not disclosed or suggested by the cited references for at least the reasons discussed above with respect to claim 1.

The claims rejected above, and depending from the above mentioned independent claims are not disclosed or suggested by the cited references at least in view of their dependencies. Furthermore, with respect to claims 4, 10 and 16, Morgan does not disclose or suggest means to indicate which mode the processor is operating. Instead, Morgan only states that the status manager repeats blocks 204 through 216 when a status change is detected for storage device (151), for example when the storage device (151) is removed from the removable media drive (121), and a new storage device is inserted. See Morgan column 6, lines 23-28. However, this does not indicate which mode the processor is operating, as recited in claims 4, 10 and 16. Therefore, for at least this additional reason, claims 4, 10 and 16 are not disclosed or suggested by the cited references.

On page 4 of the Office Action, claims 2, 6, 8, 12, 14 and 18 are rejected under 35 U.S.C. § 103(a) as unpatentable over Morgan in view of Grawrock, and further in view of Sato (U.S. Appl. Publ. No. 2001/0055980), and on page 4 of the Office Action, claims 5, 11, and 17 are rejected under 35 U.S.C. § 103(a) as unpatentable over Morgan in view of Grawrock, and further in view of Ishidera (US Patent 2002/0040442 A1).

Sato is directed to a multi-mode cellular phone terminal supporting a plurality of communication systems, which multi-mode cellular phone terminal comprises a system timer for switching over a plurality of clocks and counting different timings to support a plurality of communications system. Ishidera is directed to a software apparatus which executes processes of software with reduced power consumption at the time of operation on a battery and a recording medium. The apparatus determines whether power saving is needed or not.
The cited references fail to make up for the deficiencies in the teachings of Morgan identified above, and because all of the rejected claims ultimately depend from an independent claim, the claims are not disclosed or suggested by the cited references.

Conclusion

It is respectfully submitted that the present application is in condition for allowance, and such action is earnestly solicited. The undersigned hereby authorizes the Commissioner to charge Deposit Account No. 23-0442 for any fee deficiency required to submit this response.

Respectfully submitted,

Date: 26 July 2010

Keith R. Obert
Attorney for the Applicant
Registration No. 58,051

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
755 Main Street, P.O. Box 224
Monroe, Connecticut 06468
Telephone:(203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955